Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 63 (2015) 32 – 39

Procedia Computer Science

The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2015)

A Novel Virtual Identity Implementation for Anonymous Communication in Cloud Environments

Ibrahim A.Gomaa[a]*, Emad Abd-Elrahman[a,b]

[a]*National telecommunication Institute, 5Mahmoud El-miligy st., 6th district, Nasr City, Cairo, 11768, Egypt*
[b]*Telecom SudParis, 9 Rue Charles Fourier, Evry, 91000, France*

Abstract

This work aims at implementing new approaches for Virtual Identity (V_{Id}) in cloud environments. Our objective is to create an identity that could help in preventing the reverse of access chain in the cloud through hiding the main user identity. This means that, instead of executing a service for a known identity in cloud environment (unknown place), we hope to execute a service with an unknown identity (V_{Id}) in an unknown environment. For achieving the high degree of security and efficiency, we implement a new anonymous access for cloud environments using V_{Id}. This identity is implemented and verified using Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL library) either Identity Based Encryption (IBE) or Pseudonym Based Encryption (PBE) mechanisms. By this, a comparison between our protocols and the previous identity mechanisms used in cloud is conducted to highlight the main issues, and pros & cons for each approach.

Peer-review under responsibility of the Program Chairs

Keywords: Cloud; Virtual Environments; Virtual Identity; Security and Efficiency

1. Introduction

In Virtual environments, anonymous communication and preserving privacy are complicated tasks. Most notably cloud networking which facilitates on-demand management and control of computing, storage and connectivity resources in the network, by automatically moving or scaling up or down the resources, required to distribute content

* Corresponding author. Tel.: +2-010-011-25368; fax: +2-022-389-2140.
E-mail address: igomaa@nti.sci.eg

Peer-review under responsibility of the Program Chairs
doi:10.1016/j.procs.2015.08.309

and applications. It has at least three challenges; first of all, data confidentiality and personal information and it should be resilient in the case of security breach in which some part of the system is getting hacked [1].

Nowadays, we are experiencing an explosion in the volume of data that is created by social network users (i.e. YouTube, Facebook, Twitter ……). Those users share personal details, opinions, videos, pictures and very often their identities for each service with public or even their friends.

Therefore, the virtualized services access management over the Internet will be a critical technology for maintaining privacy and performance especially after transition to cloud computing. As keeping service provider assets secure is a strong approach to all parties, anonymous communications between users and virtual service provider became a critical issue for users to preserve their personal details.

Classically, Identity is the equivalent term for (username + password) to access any application. Later on, the Identity is developed to use some features from users like user profile (age, gender…). Moreover, it is extended to use biometric information like fingerprint and iris. This means that, the required degree of security can adjust the complexity of identity used parameters. In some applications the trusting model could be enough to run/execute an application like P2P applications, while accessing banking account could require two factor or multi-factor authentications to confirm the user's identities.

International Data Corporation (IDC) defines Identity and Access Management in the Cloud (IAM) as a comprehensive set of solutions that are used to identify users of a system and control their access to resources by associating user rights and restrictions with an established identity[2].

As users continue to depend on the virtual environments for delivery of services and more individuals are using multiple types of devices to access those services and applications, the need to hide who has access to any service will grow. Often, users suffer from password bore, having to create and remember at least one password for each service/application. Adding to the challenges of cloud networking security is the increasingly wide range of structured and unstructured data that is transferring across the network and the many types of devices used to access the network from any place. Service providers must now handle access from smart phones, tablets, PCs, and other form factors, often with different operating systems. Each device may access enterprise applications, mobile apps, social media, streaming video and traditional data each time in one access. This creates a highly sophisticated environment in which the service provider must control how and who has access to what and when.

The rest of the paper is organized as follows: in Section 2, related works will be presented and reviewed. Section 3, introduces identity challenges and work motivations. Section 4, presents the proposed virtual identity approaches. Section 5, discusses comparison and analysis for V_{Id} mechanisms. Finally, Section 6 will introduce the conclusion, and it will give future directions.

2. Related Works

This section is divided into two parts; the first one will review the identity in the cloud and the virtual environments. In the second part, the identity challenges and work motivations will be introduced, in addition to, extraction and analysis of an online survey with some questions about using identities in social networking and virtual environments[3].

2.1. Identity in the Cloud and Virtual Environments

In the Cloud Computing Technology Roadmap, the National Institute of Standards and Technology (NIST) highlighted this concern: "… the need for trusted identities and secure and efficient management of these identities while users' privacy is protected is a key element for the successful adoption of any cloud solution."[4]

Identity Management process depends on two concepts the first one is Single Sign-On (SSO) and the second one is Federated Identity Management (FIM). SSO is a possibility of a user to log in once and gain access to numerous systems or networks available in a federation without being prompted to log in again[5,6].

Federated identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains.

Numerous identity and federation manager products that support federation via Security Assertion Markup Language (SAML) versions 1.1 and 2.0 are available. Actually, there are three major protocols for federated

identity: SAML, OpenID and OAuth. SAML[7] is deployed in SSO systems, large enterprises, government agencies and service providers as their standard protocol for communicating identities across the Internet. SAML is an eXtensible Markup Language (XML)-based standard for exchanging authentication and authorization Simple Object Access Protocol (SOAP) messages between security domains, that is, between an identity provider and a service provider. Authors[8] in this work are introducing an in-depth analysis of 14 major SAML frameworks and showing that 11 of them, including Salesforce, Shibboleth, and IBM XS40, have critical XML Signature Wrapping (XSW) vulnerabilities.

OpenID is used to implement federated identity management in many web sites like Facebook, Microsoft, Google, PayPal, Symantec, and Yahoo. It is an open, decentralized user identification standard, permitting users to log onto different services with the same digital identity. In OpenID the user is authenticated using third-party services called identity providers through simple URL. Those users can choose their preferred identity providers to log in to websites that accept the OpenID authentication scheme. OpenID had a few interesting vulnerabilities like Phishing Attacks and Authentication Flaws.

OAuth is the third major open standard protocol for federated identity. It is being used exclusively for authorization purposes and not for authentication purposes like OpenID and SAML. OAuth 2.0 relies entirely on the underlying transport layer security (SSL/TLS) to provide confidentiality and integrity and does not support signature, encryption, channel binding, and client verification. Therefore, it is described as an inherently insecure protocol.

Finally, there is a growing number of other federated identity approaches. Higgins, is a new open source protocol that allows users to control which identity information is released to an enterprise or with diverse identity management systems. Windows U-Prove, is Microsoft new identity meta-system that provides interoperability between identity providers and relying parties with the user in control. MicroID, is a new identity layer to the web and micro-formats that allows anyone to simply claim verifiable ownership over their own pages and content hosted anywhere. Liberty Alliance[9], is a large commercially oriented protocol providing inter-enterprise identity trust. It is the largest existing identity trust protocol deployed around the world. SXIP[9], is commercially available product that offers users the ability to control their own identity information and authentication in use with blogs and other applications. INames[9], is a new service offering a centralized user controlled identity data store as well as providing authentication trust between enterprises. OpenSSO, is a Sun Microsystems open source version of their commercial product OpenSSO Enterprise. Ping Identity[10], Next Gen Identity platform facilitates the trusted interaction among groups of application providers and consumers on the Internet, through APIs, and from any mobile or desktop screen. AnonyControl[1] and AnonyControl-F[1] are attribute-based privilege control scheme to address the user privacy problem in a cloud storage server. Relying on various cryptographic methods, three different approaches on how the Austrian eID system based on MOA-ID could be securely moved into the cloud without violating any privacy or data protection aspects[11].

3. Identity Challenges and Work Motivations

It is convenient to use a different Virtual Identity for each service (so a different V_{Id} is used). In that way, each V_{Id} is only exposed meanwhile it is used to access to its associated service and a Virtual Identity only will contain the required attributes for accessing to one service (so less attributes will be exposed in a single access to a service).

Furthermore, V_{Id} should be a string which does not include any information about user identity, terminal being used, or service to be accessed. On that way, any sniffer attacker in the access network is only able to know the home domain of the user, but no other information.

3.1. Analysis

The aim of the survey is to develop/propose a new solution that enables personalized Identity for services, mapping Identity to user or service's needs. Through this questionnaire[3], there are a series of questions used to assess user requirements & user satisfactions and to suit their needs from using Identity over social & virtual environments. We received answers from two types of user: (users from inside our organization National Telecommunication Institute[12] and users from outside).

All target users have a good knowledge about social networking access (as the survey indicated 100%). Among them, about 70% prefer using one main identity for all social sites on base of creating one identity for each service automatically by the operators as shown in Fig. 1. (a). By this, the users are searching for an easy solution in order to avoid remembering many identities for all services. Fig. 1. (b) illustrates some questions samples and the answers globally indicate an average 70% of users are interested in privacy and virtual identity aspects.

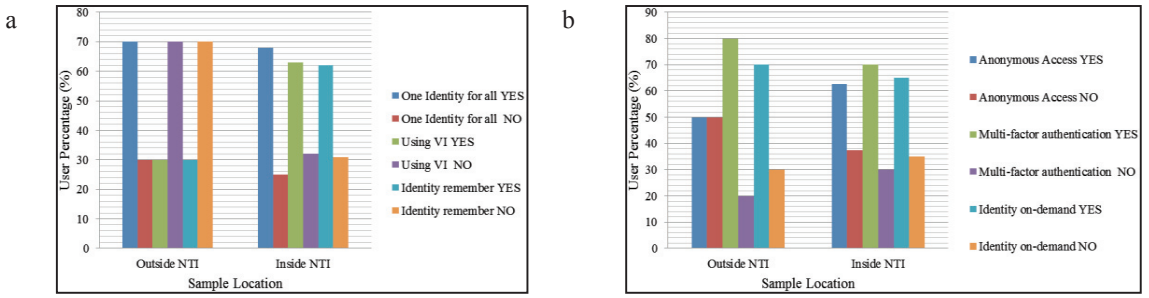

Fig. 1. (a) Samples of some identity background questions/answers in the online survey; (b) Samples of some identity security and privacy questions/answers in the online survey

4. The proposed Virtual Identity Approaches

Hereinafter, we implement two secure mechanisms for creating V_{Id}, they mainly used public-key cryptography for encryption and digital signatures. We will use Elliptic Curve Cryptography (ECC) to implement our approaches. The two solutions are common in using Private Key Generator (PKG) to calculate the V_{Id}. However, these approaches assume that a centralized Trust Authority (TA) is in charge of the private key generation. Thus, the anonymous communications are not anonymous to the TA. But, they are different in the encryption technique. We will implement the two mechanisms IBE and PBE using Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL) library[13] to evaluate the feasibility, performance and scalability of the proposed solutions. Figure 2, shows the two algorithms messages exchanges.

4.1. The First Approach: Identity Based Encryption (IBE)

Public-key based solution, such as Identity-Based Cryptographic (IBC) is an asymmetric key cryptographic technique, in which a user's public key can be an identifier of the user and the corresponding private key is created by binding the identifier with a system master secret[14].

The first approach is based on the IBC, which can be traced back to the IBE firstly proposed by Shamir[15]. The construction of the proposed IBE scheme is shown in Fig. 2. (a):

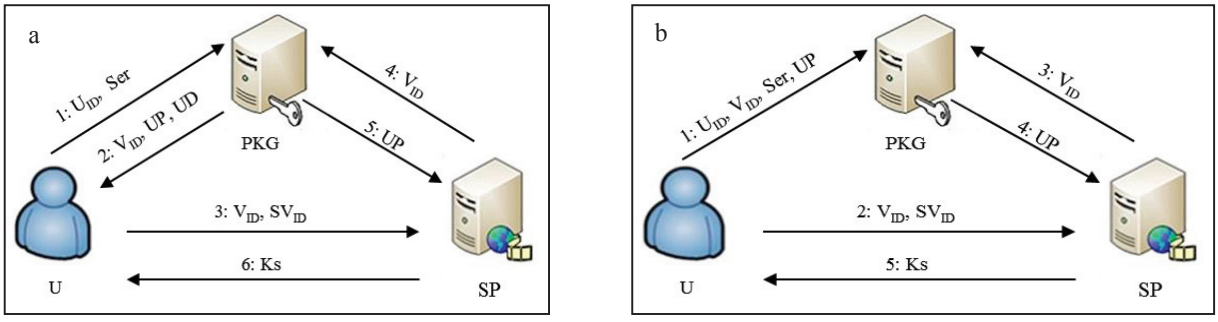

Fig. 2. (a) Proposed IBE messages exchanges; (b) Proposed PBE messages exchanges

4.1.1. Steps of IBE protocol

Since we use for this solution IBE and ECC, we have to set up the ECC parameters. The equation of the elliptic curve that we used is: $y^2 = x^3 + ax + b \ mod \ p$. The points of this curve will define a finite field; their number must be a prime number. In order to satisfy this condition, we fixed a prime number (p) and the parameter (a) in elliptic curve. And then we choose the parameter (b) in elliptic curve that satisfy this condition. We used a function in MIRACL that can calculate the number of the points in a finite field. The principle of the algorithm is as in Table 1.

Table 1. Algorithm 1: Ecpg ()

Algorithm 1: Ecpg ()
1: Choose p and a
2: Initialize b
3: Calculate n
4: if n is prime, n will be the proper parameter
Else, increase b by 1
5: go to 3

a) System setup

1- Each user send U_{ID}*: User ID* and *Ser: Requested Service to* Private Key Generator PKG.

2- The Private Key Generator (PKG) or the trust Authority (TA) selects an elliptic Curve E over GF (p) where p is a big prime number. We also denote P as the base point of E and q (big number), as the order of P.
The master Key X = (x1, x2….xn-1, xn).
The public Key Y= (y1, y2…yn-1, yn) where yi=xi*P for i=1: n.

b) Key extraction

Given U_{ID}, Ser. PKG generates V_{Id}
The Virtual Identity V_{Id} (V_{Id}=Original identity (mail, service) * Point on elliptic curve)
The User public key UP=H*V_{Id} (H is a secure hash function)
The User private key UD=S*UP (S is the master secret key of PKG)

c) Signature generation

The announcing user receives V_{Id}, UP and UD from PKG. In order to sign the user virtual identity V_{Id} using a private key UD derived from the PKG to determine V_{Id} and signature SV_{Id}, the announcing user:

1- Receives V_{Id}, UP and UD from PKG
2- Execute EcdsaSign (V_{Id}, UD) as in Table 2 to determine SV_{Id}.

Table 2. Algorithm 2: EcdsaSign (V_{Id}, UD)

Algorithm 2: EcdsaSign (V_{Id}, UD)
1: Generate n a large prime number
2: Calculate d= UD mod (n-2)
3: Computes Q = d* UP
4: Select a statistically unique and unpredictable integer k in the interval [1, n-1].
5: Compute k* UP = (x1, y1) and r = x1 mod n. If r = 0, then go to 4. (This is a security condition: if r = 0, then the signing equation:
$s = k^{-1}*(H(V_{Id}) + d*r) \ mod \ n$ does not involve the private key d).
6: Compute k^-1 mod n.
7: Compute $s = k^{-1}*(h(V_{Id}) + d*r) \ mod \ n$ where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go to 4. (If s = 0, then s^{-1} mod n does not exist; s^{-1} is required in iteration 2 of the signature verification.)
8: The signature for the discovery message m is the pair of integers (r, s) = Sig (V_{Id}).
9: Return Sig (V_{Id}) = (r, s)
10: Publish (Sig (V_{Id}), n, Q)

d) *Signature Verification*

Once the service provider receives the signed virtual identity V_{Id}, it asks PKG for the public key for checking the signed virtual identity SV_{Id} , Algorithm steps are given in Table 3.

Table 3. EcdsaVer (V_{Id}, UP)

Algorithm 3: EcdsaVer (V_{Id}, UP)
1: Verify that r and s are integers in the interval [1, n-1].
2: Compute $w = s^{-1}$ mod n and $h(V_{Id})$.
3: Compute $u1 = h(V_{Id})*w$ mod n and $u2 = r*w$ mod n
4: Compute $u1*UP + u2*Q = (x0, y0)$ and $v = x0$ mod n.
5: Accept the signature if and only if v=r.

e) Encrypt future communication

If the verification of the signature is successful, the service provider SP generates Shared Secret Key *Ks* and sends it to user U. Otherwise it is discarded.

After generate the pre-shared key Ks, We denote encrypting future communication (i.e, a message m) using pre-shared key Ks as EcdhEncrypt (m), Algorithm 4, Table 4. The resulting ciphertext is denoted by c. The decryption of ciphertext c using the same pre-shared key Ks is given as EcdhDecrypt(c), Algorithm 5, Table 4.

Table 4 Algorithm 4: EcdhEncrypt (m); Algorithm 5: EcdhDecrypt (c)

Algorithm 4: EcdhEncrypt (m) [Encrypt future communication]	Algorithm 5: EcdhDecrypt (c) [Decrypt future communication]
1: Generate a random number a ∈ GF (p).	1: Generate a random number b ∈ GF (p).
2: Calculate multi_a= a.UP	2: Calculate multi_b= b.UP
3: Publish (multi_a)	3: Publish (multi_b)
4: Receive multi_b	4: Receive multi_a
5: Calculate Ks=a*multi_b	5: Calculate Ks=b*multi_a
6: Encrypt m with Ks, {m} Ks	6: Encrypt m with Ks, {m} Ks
7: Return c= {m} Ks	7: Return {m} Ks

4.2. The Second Approach: Pseudonym Based Encryption (PBE)

The second approach is based on Pseudonym Based Encryption, which was proposed for Key management for anonymous communication in mobile ad-hoc networks[16]. In this approach, user uses Pseudonym Based Encryption to calculate its own V_{Id}. The PKG will just compute the user's private key which depends on its secret master key. The PKG will act as an authority which certifies that the user has the private key corresponding to his/her public key. Fig. 2.(b) shows PBE messages exchanges.

The user sends to the PKG his/her identity (e.g., user@homeoperator.com), the requested service, the public key by choosing an ECC with a point P a generator of it and chooses his/her V_{Id} (as pseudonym). The PKG calculates the user's private key UD and will not send the key pair (public/private) to the user because the UP and UD are already computed by the user. The user wants to be authenticated by SP; therefore he/she uses an Identity Based Signature (IBS)[15] to calculate SV_{Id} and sends it with V_{Id} to the SP. The SP sends V_{Id} to the PKG and asks for public key corresponding to the V_{Id}. The SP verifies the SV_{Id} by decrypting it using the UP. If it retrieves the V_{Id}, then the authentication succeeds. At the end, the SP generates and sends a shared secret key to the user to encrypt future communication between them.

We will implement the PBE using the same steps as done before in IBE except for the second step in IBE (as the trusting verified by the cloud service provider in this case).

1- Each user sends U_{ID}: *User ID and Ser: Requested Service* V_{Id}: *Virtual ID (Pseudonym), UP: User Public Key* to Private Key Generator PKG. The PKG is in charge of the private key generation within an anonymous communication system. Therefore, the anonymous communications are not anonymous to the trust authority (TA).
2- The Private Key Generator (PKG) or the trust Authority (TA) will just compute the user's private key which depends on its secret master key. PKG selects an elliptic Curve E over GF (p) where p is a big prime number. The PKG calculates the user's private key UD and will not send the key pair (public/private) to the user because the UP and UD are already computed by the user.

Other steps will follow the same steps as described before in IBE.

5. Approaches Comparison & Analysis

As mentioned before about Federated Identity (FI) and password management, the three major protocols for federated identity are not yet suitable for providing the high level of security and reliability to satisfy authentication demanded by important services such as financial institutions, governments, mobile operators and public services. Therefore, Table 5 shows the comparison between our proposed approaches and major protocols of federated identity.

Table 5. Comparison between proposed approaches and major FI protocols

Protocols / Security Consideration		Federated Identity Protocols			Proposed Protocols	
		OpenID	SAML	OAuth	IBE	PBE
Authentication		Using identity provider and Controlled by relying party	Exchanging XML messages between service provider and identity provider	Not for authentication purpose.	Trusting between PKG and service provider	Handshaking between PKG and service provider
Rekeying	Forward Secrecy	Compromised by phishing attacks and authentication flaws	Compromised by XML signature wrapping vulnerabilities	Session fixation vulnerability flaw, does not support client verification and signature	Dynamic policy updating through PKG	Randomization of value K each login
	Backward Secrecy				Irreversible to main identity	Using identity based signature
Main Purpose		SSO for Consumers	SSO for enterprise users	API authorization between apps	SSO and anonymous communication	SSO and anonymous communication
Overhead and complexity		10 messages for handshaking	6 messages for handshaking	10 messages for handshaking	6 messages for handshaking	5 messages for handshaking
Dates From		2005	2001	2006	2015	2015
No. of related CVEs		24	17	3	None	None
Protocols used		XRDS, HTTP	SAM,XML,HTTP ,SOAP	JSON, HTTP	HTTPS, SSL, Elliptic Curve	HTTPS, SSL, Elliptic Curve

5.1. Security and Performance

The proposed work uses IBC + ECC for Master Key and Private Key Generation. Therefore, our approaches increase the level of security in order to prevent any form of attack and guarantees;

- Non-Repudiation, Integrity, Privacy and Anonymity (ECC is based on pseudonym instead of identity which leads to assure privacy, anonymity and solve identity disclosure problem),
- Dynamicity (It is assured by re-generate virtual identity for each service) and Identity Disclosure.

5.2. Scalability

The results we got to create V_{Id} is around 40 ms and 32 ms for the principal functions for IBE and PBE respectively, using a computer machine (Intel Core 2 Duo CPU E8400 @ 3.00GHz x 2, memory 4G in Linux Ubuntu 12.10). We evaluated the time needed to create the V_{Id} by different number of users. Table 6 shows the results.

Table 6. IBE and PBE scalability

Number of users	V_{Id} creation time IBE	V_{Id} creation time PBE
1000	40 S	32 S
5000	200 S	160 S
10000	400 S	320 S
50000	2000 S	1600 S

6. Conclusion and Future Work

This paper showed numerous features for VId and identity management in different environments to eliminate the need to maintain distinct user credentials for separate applications, therefore simplified administration and streamlined access to resources are satisfied. We suggest two protocols IBE and PBE for SSO and anonymous communication to help Cloud and Internet users to protect their privacy and private information from any disclosure. Furthermore, the paper conducts comparison and analysis between the proposed approaches and three major protocols for federated identity OpenID, SAML and OAuth. The features and advantages of the proposed protocols over the standard protocols are mentioned. One of the promising future works is to extend our solutions to include group communication and design security model to compare quantitatively the IBE and PBE with the approaches of related works.

References

1. Taeho Jung, Xiang-Yang Li, Zhigu Wan and Meng Wan, “Control Cloud Data Access Privilege and Anonymity with fully Anonymous Attribute-Based Encryption”, *IEEE transaction on information forensics and security*, VOL.10, NO.1, January 2015.
2. Hudson S., and Grady J., “Eliminating Authentication Silos and Password Fatigue with Federated Identity and Access Management”, Adapted from Worldwide Identity and Access Management 2012 – 2016 *Forecast: Growth Driven by Security, Cloud and Compliance*, IDC #238553.
3. Survey about using Identities in Social Networks and Virtual Environments, *http://www.ntiegypt.sci.eg/survey/index.php/212212/*, last visit: May 2015.
4. National Institute of Standards and Technology (NIST), Computer Security Division, *Information Technology Laboratory*, July 2013.
5. Galpin R. and Flowerday S., “Online Social networks: Enhancing user trust through effective controls and identity management”, *IEEE,* 2011.
6. Hamlen K., Liu P., Kantarcioglu M., Thuraisingham B. and Yu T., “Identity Managemnet for Cloud Computing: Developments and Directions”, *CSIIRW ’11*, October 12 -14, 2011.
7. Prasanalakshmi B. and Kannammal A., “Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics”, *International Journal of Computer Applications*, Volume 53, No.18, September 2012.
8. Somorovsky J., Mayer A., Jorg S., Schwenk j., Kampmann M., and Jensen M., “On Breaking SAML: Be Whoever You Want to Be”, *21st USENIX Security Symposium*, August 8-10, 2012.
9. Authentication world, *http://www.authenticationworld.com/Authentication-Federation,* last visit: May, 2015
10. Ping Identity, *https://www.pingidentity.com/en/products/next-gen-identity.html,* last visit: May, 2015
11. Please cite this article in press as: Zwattendorfer B, Slamanig D, Design strategies for a privacy-friendly Austrian eID system in the public cloud, Computers & Security (2015 Elsevier Ltd.), http://dx.doi.org/10.1016/j.cose.2015.03.002
12. National Telecommunication Institute, http://www.nti.sci.eg/, last visit: May, 2015.
13. Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL) library, *http://www.certivox.com/miracl/*, last visit: May, 2015
14. Chen L., “An Interpretation of Identity-Based Cryptography”, Foundations of Security Analysis and Design IV, *Lecture Notes in Computer Science*, Volume 4677, 2007.
15. Boneh D. and Franklin M., “Identity-Based Encryption from the Weil Pairing”, *CRYPTO 2001*, LNCS 2139, Springer-Verlag, 2001.
16. Huang D., “Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks”, Int. J. Security and Networks, Vol. 2, 2007.